

This Document can be made available in alternative formats upon request

State of Minnesota

HOUSE OF REPRESENTATIVES

EIGHTY-NINTH SESSION

H. F. No. 2385

03/08/2016 Authored by Lesch, Metsa, Schultz, Davnie and Pugh

The bill was read for the first time and referred to the Committee on Civil Law and Data Practices

1.1 A bill for an act
1.2 relating to data privacy; protecting applicant's and employee's personal
1.3 usernames and passwords from access by employers; providing for civil
1.4 enforcement; proposing coding for new law in Minnesota Statutes, chapter 181.

1.5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.6 Section 1. **[181.990] EMPLOYEE USERNAME AND PASSWORD PRIVACY**
1.7 **PROTECTION.**

1.8 Subdivision 1. **Definitions.** (a) For the purposes of this section, the following terms
1.9 have the meanings given them in this subdivision.

1.10 (b) "Applicant" means an applicant for employment.

1.11 (c) "Employee" means an individual who provides services or labor for an employer
1.12 for wages or other remuneration.

1.13 (d) "Employer" means a person who is acting directly as an employer, or indirectly in
1.14 the interest of an employer, on behalf of a for-profit, nonprofit, charitable, governmental,
1.15 or other organized entity in relation to an employee.

1.16 (e) "Personal social media account" means an account with an electronic medium
1.17 or service where users may create, share, and view user-generated content, including,
1.18 but not limited to, uploading or downloading videos or still photographs, blogs, video
1.19 blogs, podcasts, messages, e-mails, or Internet Web site profiles or locations. Personal
1.20 social media account does not include: (1) an account opened at an employer's behest,
1.21 or provided by an employer, and intended to be used solely on behalf of the employer,
1.22 or (2) an account opened at a school's behest, or provided by a school, and intended
1.23 to be used solely on behalf of the school.

2.1 (f) "Specific content" means data or information on a personal social media account
2.2 that is identified with sufficient particularity to:

2.3 (1) demonstrate prior knowledge of the content's details; and

2.4 (2) distinguish the content from other data or information on the account with which
2.5 it may share similar characteristics.

2.6 Subd. 2. **Employer access prohibited.** An employer shall not:

2.7 (1) require, request, or coerce an employee or applicant to disclose the username,
2.8 password, or any other means of authentication, or to provide access through the username
2.9 or password, to a personal social media account;

2.10 (2) require, request, or coerce an employee or applicant to access a personal social
2.11 media account in the presence of the employer in a manner that enables the employer
2.12 to observe the contents of the account; or

2.13 (3) compel an employee or applicant to add any person, including the employer, to
2.14 their list of contacts associated with a personal social media account or require, request, or
2.15 otherwise coerce an employee or applicant to change the settings that affect a third party's
2.16 ability to view the contents of a personal social networking account.

2.17 Subd. 3. **Employer actions prohibited.** An employer shall not:

2.18 (1) take any action or threaten to take any action to discharge, discipline, or otherwise
2.19 penalize an employee for an employee's refusal to disclose any information specified in
2.20 subdivision 2, clause (1), for refusal to take any action specified in subdivision 2, clause
2.21 (2), or for refusal to add the employer to their list of contacts associated with a personal
2.22 social media account or to change the settings that affect a third party's ability to view the
2.23 contents of a personal social media account, as specified in subdivision 2, clause (3); or

2.24 (2) fail or refuse to hire any applicant as a result of the applicant's refusal to disclose
2.25 any information specified in subdivision 2, clause (1), for refusal to take any action
2.26 specified in subdivision 2, clause (2), or for refusal to add the employer to their list of
2.27 contacts associated with a personal social media account or to change the settings that
2.28 affect a third party's ability to view the contents of a personal social media account, as
2.29 specified in subdivision 2, clause (3).

2.30 Subd. 4. **Employer actions permitted.** Nothing in this section shall prevent an
2.31 employer from:

2.32 (1) accessing information about an employee or applicant that is publicly available;

2.33 (2) complying with state and federal laws, rules, and regulations and the rules of
2.34 self-regulatory organizations, where applicable;

2.35 (3) requesting or requiring an employee or applicant to share specific content
2.36 that has been reported to the employer, without requesting or requiring an employee or

3.1 applicant to provide a username, password, or other means of authentication that provides
 3.2 access to a personal social media account, for the purpose of:

3.3 (i) ensuring compliance with applicable laws or regulatory requirements;

3.4 (ii) investigating an allegation, based on receipt of specific information, of the
 3.5 unauthorized transfer of an employer's proprietary or confidential information or financial
 3.6 data to an employee or applicant's personal social media account; or

3.7 (iii) investigating an allegation, based on receipt of specific information, of unlawful
 3.8 harassment in the workplace;

3.9 (4) prohibiting an employee or applicant from using a personal social media account
 3.10 for business purposes; or

3.11 (5) prohibiting an employee or applicant from accessing or operating a personal
 3.12 social media account during business hours or while on business property.

3.13 Subd. 5. **Employer protected if access inadvertent; use prohibited.** If an
 3.14 employer inadvertently receives the username, password, or other means of authentication
 3.15 that provides access to a personal social media account of an employee or applicant
 3.16 through the use of an otherwise lawful virus scan or firewall that monitors the employer's
 3.17 network or employer-provided devices, the employer is not liable for having the
 3.18 information, but may not use the information to access the personal social media account
 3.19 of the employee or applicant, may not share the information with anyone, and must delete
 3.20 the information immediately or as soon as is reasonably practicable.

3.21 Subd. 6. **Enforcement.** Any employer or educational institution, including its
 3.22 employee or agents, that violates this section shall be subject to legal action for damages
 3.23 or equitable relief, to be brought by any other person claiming a violation of this section
 3.24 has injured the person or the person's reputation. A person so injured shall be entitled to
 3.25 actual damages, including mental pain and suffering endured on account of violation of
 3.26 the provisions of this section, and reasonable attorney fees and other costs of litigation.

3.27 Subd. 7. **Severability.** The provisions in this section are severable. If any part
 3.28 or provision of this section, or the application of this section to any person, entity, or
 3.29 circumstance, is held invalid, the remainder of this section, including the application of
 3.30 the part or provision to other persons, entities, or circumstances, shall not be affected by
 3.31 the holding and shall continue to have force and effect.

3.32 **EFFECTIVE DATE.** This section is effective the day following final enactment.